



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,687	06/20/2003	Philip D. MacKenzie	15	6727
<div>7590 10/11/2007</div> <div>Ryan, Mason, & Lewis, LLP 90 Forest Avenue Locust Valley, NY 11560</div>				
			EXAMINER	
			TO, BAOTRAN N	
			ART UNIT	PAPER NUMBER
			2135	
			MAIL DATE	DELIVERY MODE
			10/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No. 10/600,687	Applicant(s) MACKENZIE, PHILIP D.	
	Examiner Bao Tran N. To	Art Unit 2135	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 September 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) ☐ They raise the issue of new matter (see NOTE below);
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: NONE.
Claim(s) objected to: NONE.
Claim(s) rejected: 1-16.
Claim(s) withdrawn from consideration: NONE.

IN PART

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____.
13. ☐ Other: _____.

DETAILED ACTION

Continuation of 3: Claims 8 and 16 are not entered because the applicant proposes to amend independent claims 8 and 16. The amended limitations raise new issues that would require further consideration and search.

Continuation of 11: Claims 1-7 and 9-15 are entered because the request for reconsideration has been considered but does NOT place the application in condition for allowance because: Applicant's arguments filed 09/26/2007 have been fully considered but they are not persuasive.

Applicant argues, "Applicant submits that the Examiner has failed to establish a proper case of obviousness in the §103(a) rejection of claims 1, 2, 4-6, 9, 10 and 12-14 over Cramer and Faucher, in that the Cramer and Faucher references, even if assumed to be combinable, fail to teach or suggest all the claim limitations, and in that no cogent motivation has been identified for combining the references or modifying the reference teachings to reach the claimed invention" (Page 2 of Remarks).

Examiner respectfully disagrees with this contention. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21

Art Unit: 2135

USPQ2d 1941 (Fed. Cir. 1992), In this case, Cramer's reference and Faucher's reference are analogous arts. They both specifically disclose to how to secure communications by using the cryptographic system that can support the motivation to combine the Cramer's teaching with Faucher's teaching to establish the limitations of Claim 1 that provides secure communications conducted over insecure channels (Faucher, col. 1, lines 13-15). Furthermore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using public-keys method (Faucher, col. 1, lines 13-15).

Applicant argues, "No where does Cramer teach or suggest the recited limitation of 'generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party, device to the first party device.' Again, as noted-above, the first and second devices can jointly decrypt a ciphertext, but neither can decrypt a ciphertext alone, such that the first and second

Art Unit: 2135

devices communicate with each other to decrypt the ciphertexts, which Cramer does not disclose" (Page 3 of Remarks).

Examiner respectfully disagrees with applicant. Examiner would like to point out that the applicant made a mistake to the above argument. Claims 1 is rejected under 35 U.S.C. 103(a) unpatentable over Carmer and Faucher. Carmer explicitly discloses the step of generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second device, (Col. 8 line 25 to Col. 10 line 5) {Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender} (Cramer and Shoup cryptographic system invention).

Cramer explicitly does not disclose "wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device."

However, Faucher explicitly discloses wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device (col. 3, lines 5-50).

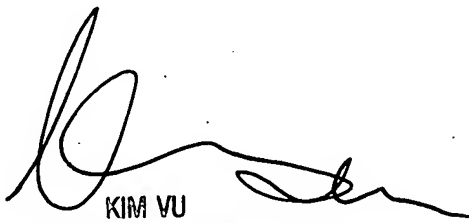
Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext

Art Unit: 2135

from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using public-keys method (Faucher, col. 1, lines 13-15).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the first and second devices can jointly decrypt a ciphertext, but neither can decrypt a ciphertext alone, such that the first and second devices communicate with each other to decrypt the ciphertexts) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

For at least the above reasons, it is believed that the rejection is maintained.



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100